BNA, INC.

PRIVACY & SECURITY LAW

BNA Employee-Owned Since 1947

REPORT

FTC Releases Draft Privacy Report: Analysis and Implications for 2011 and Beyond

BY REED FREEMAN AND JULIE O'NEILL

Last week, the Federal Trade Commission (FTC or Commission), by a vote of 5-0, released its long-awaited staff report on privacy, ''Protecting Consumer Privacy in an Era of Rapid Change.''[1]

Based largely on themes and concepts developed through a series of privacy roundtables held by the Commission in 2009 and 2010, the staff report sets out an exhaustive proposed framework for how companies should protect consumers' privacy. However, while breathtaking in its scope and detail, the report leaves more questions than answers. First among those questions is which elements of the proposed framework are required by Section 5 of the FTC Act and which are aspirational? The Commission has used its bully pulpit to lay out how companies should promote consumer privacy, but it will fall short of its ambition of turning those aspirations into practice unless it lets industry know where the Section 5 line is. Comments are due by Jan. 31, 2011, and the Commission expects to release a final report, which may be more concrete, later in 2011.

The proposed framework begins with a nearly universal scope. According to the Commission, ''[t]he proposed framework would apply broadly to online and offline commercial entities that collect, maintain, share, or otherwise use consumer data that can reasonably be linked to a specific consumer, computer, or device.''[2] Given the Commission's skepticism regarding the likelihood that anonymous data can be presumed to remain

[1] The report is here: http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.

Reed Freeman is a partner and Julie O'Neill is Of Counsel in Morrison & Foerster LLP's Washington office.

[2] *See id.* at v.

 ISSN 1538-3423

anonymous,[3] it is difficult to imagine an entity or piece of data that would not fall within this scope. Conspicuously absent is any concept that certain entities performing services for a first party, at the direction of the first party, and with no independent rights to the data (generally referred to as vendors or service providers), should be exempt. Congressional privacy bills from the 111th Congress recognized such an exemption. Nor does the Commission make any attempt to say what data elements are not included. Aggregate data should qualify, but we have no assurance of that, given that it is derived from user-level data.

The Commission's proposed framework consists of three major elements: (1) privacy by design, (2) simplified consumer choice, and (3) greater transparency.

1. Privacy By Design

The framework proposes that organizations bake privacy into their business practices through a concept dubbed ''privacy by design.'' In practical terms, this means following a version of the fair information practices that advocates have been calling for as core elements of baseline privacy legislation. As a group, these practices appear to be recommended best practices rather than new requirements under Section 5. Individually, however, some of these recommendations, such as reasonable security and secure disposal, are already considered by the Commission to be required under Section 5.

Elements of Privacy By Design

According to the report, a company should incorporate substantive privacy protections into its everyday practices. These protections include: (1) providing reasonable security for consumer data, (2) collecting only the data needed for a specific business purpose, (3) retaining data only as long as necessary to fulfill that purpose, and (4) implementing reasonable procedures to promote data accuracy.

Reasonable security and limited data retention have long been Commission maxims, and there is nothing new there. Promoting data accuracy is not law today outside certain regulated industries, but presumably companies have an incentive to do so for their own commercial reasons.

What *is* new here? Limiting companies to collecting data only for a purpose specified at the point of collection is not law today, and it may require some companies to make changes to what they collect or what they disclose at the point of collection. The concept is sound, but it is difficult to apply in practice and comes with costs. The case on the margin involves the collection of data for one purpose and the use of it later for a purpose that may not be material to the consumer, such as site optimization or retail store design. There are nearly unlimited ways a company may choose to use data after it has collected it, and a restriction on all such uses seems too restrictive. Clearly, work needs to be done here to provide organizations with flexibility without imposing on consumers' privacy expectations.

[3] The Commission explains that this approach is supported by the fading of the traditional personally identifiable information (PII)/non-PII distinction, ''due to changes in technology and the ability to re-identify consumers from supposedly anonymous data.''

The Commission proposes a bifurcated framework for ways companies can make data choices more prominent, relevant and easier for consumers.

The framework also proposes that a company should maintain comprehensive data management procedures throughout the life cycle of its products and services. This means that it should develop, implement, and enforce a comprehensive privacy program, tailored in size and scope to the risks presented to the data it processes. A company should also designate personnel to train employees, promote accountability, and periodically review the program. Among other things, according to the report, an appropriate program should ensure that privacy and data security are taken into account in the early stages of development and throughout the lifecycle of the resulting product or service.

This concept is new to privacy in the United States, at least as a legal requirement under Section 5 imposed across industries, and it would come with substantial costs. It is a direct descendant of the Commission's data security cases, where Commission orders have required companies to engage in security training, designate employees responsible for an information security program, and audit their security practices over time. This includes the hiring of additional personnel to conduct what amounts to initial and, thereafter, regular privacy audits, for all products and services that involve data collection. All of this would have to be documented, of course, amounting to another layer of the auditing and recordkeeping requirements with which companies are already struggling. The Commission acknowledges that there is a sliding scale for this new concept, but it may make more sense to tie this requirement, if indeed it is or becomes one, to sensitive data. It would be overly burdensome for the potential gain, for example, to apply it to non-personal data collected for first-party analytical purposes.

2. Simplified Consumer Choice

The framework sets forth ways in which companies should make data choices more prominent, relevant, and easily accessible to consumers. The Commission proposes a bifurcated framework depending on whether the collection or use is ''commonly accepted'' by consumers.

Commonly accepted practices get a free pass: no explicit consent is required because it can be inferred. The logic behind this is that because such practices are obvious in context, the consumer understands and agrees to them. To enjoy this type of treatment, it follows that this category of uses must necessarily be narrow. Examples provided by the Commission include product and service fulfillment, internal operations, fraud prevention, legal compliance, and first-party marketing. Clearly, because this category results in implied consent, the comments from stakeholders are likely to focus on which types of uses are and are not ''commonly accepted.'' This is a crucial issue, and it is therefore important for companies to review their data practices to determine which merit treatment as ''commonly ac-

  PVLR ISSN 1538-3423

cepted'' in context under this paradigm, and to make those arguments in their comments.

There are inherent problems with this paradigm. What is or is not ''commonly accepted'' is a subjective determination. If this portion of the framework becomes final without more guidance, companies will be taking some risk every time they determine something is commonly accepted. That creates an incentive not to rely on it, which in turn defeats the entire purpose of this exception. If the Commission sticks with this framework, the market will need much more guidance, and that guidance will need to be refreshed periodically. No one knows better than the Commission that the market abhors a vacuum.

Uses and disclosures that are not ''commonly accepted'' would require meaningful choice. This means outside of the privacy policy and easy for the consumer to see, understand, and execute. Examples of these practices include sharing with a third party for its own marketing or other purposes and social media services where the service provider permits third-party applications to collect users' data. Because these uses and disclosures are not obvious to a consumer, the Commission argues, his or her consent to them cannot be inferred; rather, the company must obtain it.

There are other problems with this paradigm. If the treatment of uses and disclosures bears a resemblance to the Commission's ''clear and conspicuous'' standard, then the implication is that all uses and disclosures that are not ''commonly accepted'' are material. That begs the question: why did the Commission not use the term ''material,'' which has generations of interpretation, guidance, and caselaw behind it? Does the Commission mean to impose a standard for material disclosures for uses and disclosures that fall short of being material to consumers? If that's the case, then this report represents a sea-change for the Commission and a slippery slope. Once the materiality wall is torn down, there are implications throughout the entire body of consumer protection law. The threshold for materiality is high, and for good reason: material disclosures must be clear and conspicuous. If all disclosures must be clear and conspicuous, then the entire disclosure regime becomes a confusing, cluttered mess.

The problem is especially apparent in privacy. Notwithstanding the Commission's ''commonly accepted'' dichotomy, the world is not so neat, and there are many things that fall into the grey area between ''commonly accepted'' and ''not commonly accepted.'' If companies are incented by fear of enforcement action to treat most uses and disclosures as not commonly accepted, then consumers will be inundated with requests for consent and likely to give up. A better framework is materiality because the market knows what that means.

The report next moves to how choices should be offered. To be most effective, the Commission suggests that choices should be clearly and concisely described and offered when—and in a context in which—the consumer is making a decision about his or her data. This allows for the ''just in time'' notice, whereby a company presents the choice to the consumer at the point at which he or she enters personal data (such as in an online retail transaction) or accepts a product or service (such as at checkout in an offline transaction). The question is whether it not just permits that type of notice but instead mandates it. Again, the danger is choice exhaustion.

The Commission's report punts on whether and when a notice should be opt-out or opt-in—another concrete piece of guidance that businesses need. It does suggest that opt-in is required for uses of sensitive data (ignoring that some such uses may be commonly accepted), but it also punts on how that term should be defined. It has requested comment on this and other issues, so the final framework may provide guidance.

Notwithstanding the problems inherent in the ''commonly accepted''/''not commonly accepted'' dichotomy, it is likely that this portion of the Commission's preliminary report will result in enforcement actions in the near term. Requiring clear notice and choice for nonobvious aspects of a company's data collection practices has its roots in the FTC spyware cases of the early 2000s. The Commission has maintained this position since then, most recently enforcing it in the context of alleged data transfers to third parties disclosed deep within a company's End User License Agreement.[4]

Support for a Do Not Track Mechanism

The Commission has taken the position that the most ''practical'' way to offer consumers choice in the context of online behavioral advertising is via a universal do not track mechanism. According to the Commission, this would most likely involve the placement of a persistent setting, similar to a cookie, on the consumer's browser, signaling his or her choices about being tracked online. The Commission seeks comments on a variety of issues related to this proposal, including whether any such mechanism should offer consumers granular options (*e.g.*, to control the types of advertising they receive or the types of data collected about them).

The Commission's report punts on whether and when a notice should be opt-out or opt-in—another concrete piece of guidance that businesses need.

The Commission is careful to note that it does not believe that it has the legal authority to develop and implement a do not track requirement and suggests that it must be done by either the private sector or through legislation. Already, some members of Congress have suggested that they support some form of do not track legislation. It is not clear whether such legislation will move in the 112th Congress. Nor is it clear that a broad-based, industry-developed do not track program will emerge any time soon. It is more likely that individual companies will compete to offer their own, private, do not track programs and seek to build large audiences of subscribers among web publishers and advertisers who may feel an incentive to subscribe to protect their brands. These efforts could consolidate, they could exist side-by-side in the market, or, eventually, one may emerge as a market leader. In any event, it is not un-

[4] *See FTC v. EchoMetrix, Inc.*, CV10-5516 (E.D.N.Y. Nov. 30, 2010). Full text of the stipulated final order is available at http://op.bna.com/pl.nsf/r?Open=dapn-8bsjb2.

likely that the market will work to address this Commission concern, driven by an incentive brands continue to feel to be privacy friendly.

While a do not track mechanism has bumper sticker appeal and echoes of the Commission's popular do-not-call list, it is still at the whiteboard stage. The Commission can only describe how it would work in broad strokes. The issues are complex, and the Commission proposes to make them even more complex by offering granular choices. What if consumers ignore it? On the other hand, what if consumers flock to it? If that were to happen, what would the implications be for the free internet as we know it? No one knows the answer to these questions, but they are important, to say the least.

3. Greater Transparency

The framework proposes a variety of measures aimed at improving the transparency to consumers of companies' data practices. Specifically, according to the report, companies should make their privacy policies clearer, shorter, and standardized, so that a consumer can understand them more easily and be able to compare them across companies. At this time, the Commission has not proposed any particular standardized format, although it has noted work on standardized notices in the Gramm-Leach-Bliley Act context as a possible guidepost. Nor has the Commission made clear that it intends to enforce Section 5 against companies for failure to standardize their privacy policies, or even to make them clearer.

The Commission also proposes that companies provide consumers with reasonable access—based on the costs and benefits of access in a particular situation—to the data they hold about them. This applies even to companies that do not interact directly with consumers, such as data brokers. The Commission has asked for comment on the feasibility of this, but it is clearly something it wants to encourage, if not one day mandate. Whether it is feasible or, instead, intended as technology-forcing should become clearer in the final report.

The Commission also reiterates a theme to which it has stuck since 2004: companies must provide robust notice and obtain express consent before using consumer data in a materially different way than claimed when the data was collected. This proposal is consistent with the Commission's enforcement activity and prior industry guidance.[5] Still, one wonders whether this requirement in and of itself remedies an unfair practice Under the Commission's unfairness test, a practice is unlawful if it imposes substantial harm on consumers, is not avoidable by consumers, and is not outweighed by benefits to consumers or competition. In this context, the Commission struggles to articulate a cognizable harm. If there is one, it would be unavoidable without clear notice, but not necessarily without opt-in consent. Indeed, the Commission itself recognized in its report that some opt-out consents are more consumer-friendly than some opt-in consents. Finally, and most importantly, can the Commission defend in every case the assertion that the marginal privacy gain by obtaining an opt-in outweighs the costs to competition by forcing companies to create and maintain separate databases of consumers, segregated by privacy policy version?

Conclusion

Overall, the Commission's report reflects its concern that consumers bear too much burden for understanding and controlling how their data is collected, used, retained, and disclosed, and its desire to see this paradigm reversed. The report contains some novel ideas but is a long way from being in a position to achieve one of its core missions, which is to provide concrete and meaningful guidance to the business community. How far the Commission goes in accomplishing that mission will depend in large part on the comments it receives.

---

[5] *See, e.g., Gateway Learning Corp.*, No. C-4120, 2004 WL 2618647 (FTC Sept. 10, 2004); OBA Report, note 37.

  PVLR ISSN 1538-3423